安全事件回應 (IR)

通常而言，信息安全事件是在沒有警告的情況下發生。即使被發現，企業亦可能沒有足夠的資源或知識來有效地處理攻擊事件，從而造成巨大和持續的損失。中信國際電訊CPC的信息安全事件回應服務 (IR)擁有 24x7x365 訓練有素的信息安全團隊，可提供快速回應，及時採取專業行動，為客戶調查和防止攻擊。解決事情後，我們的團隊會向客戶提供詳細的"事後報告"。

產品特點

- 24x7x365專責安全事件回應團隊迅速地處理信息安全事件調查、規劃補救方法和減少攻擊。
- 提供記憶體和硬碟的取證，及詳細的報告去闡述方法和發現，以供管理層或法律上的參考。
- 提供詳細"事後報告"，包括根本原因的分析、程序的檢討、得著和見解及改進的建議。
- 提供自適應的回應框架，以啟動自動化工作流程。

端點偵測及回應服務 (EDR)

TrustCSI™ 端點偵測及回應服務 (TrustCSI™ EDR) 是一個完整的端點安全解決方案，專為新的業務時代而構建。它在復雜的現代威脅環境中提供實時企業保護。各種迫在眉睫的端點威脅（例如網絡釣魚、勒索軟件和惡意軟件）可以通過自動偵測及修復功能，減低資訊安全風險。借TrustCSI™ EDR為整個企業網絡提供威脅偵測監控，優化回應率以加快威脅偵測和回應速度，並進一步擴展服務能力，保護所有端點。

重點

- 預防網絡攻擊以免造成損害：服務運用新一代防毒（NGAV）、反惡意軟件、反網絡釣魚、沙盒、內容威脅解除與重組等技術，協助企業主動阻止網絡攻擊避免造成任何損害。
- 實現實時偵測和保護：服務具有備用的行為分析、反勒索軟件、防漏洞及其他技術，企業可以更有效修復由勒索軟件、惡意軟件及無檔案攻擊等各類網絡攻擊造成的影響。全自動化修復功能即使在離線狀態下亦可發揮作用。
- 改善攻擊偵查和回應：自動產生詳盡的鑑證報告，協助系統管理員和事件回應小組分析系統的健康狀態。透過強大的攻擊診斷功能，事件回應小組可快捷有效地採取相應行動，解決網絡攻擊問題。
- 利用自動化以增加修復數量：服務根據預設規則，自動對既定事件作出回應行動，阻截或迅速修復特定事件，減低事件回應小組的工作量。
- 24x7 信息安全運作中心（SOC）託管及監控服務：中信國際電訊CPC的網絡保安專家提供全天候監控及託管服務，以偵測及預防端點遭受的網絡攻擊，並同提作出準確及時的預警。

中信國際電訊CPC
CITIC TELECOM CPC

TrustCSI™ 3.0

威脅偵測及回應服務

透過精確的準度和可用性防護您的企業

中信國際電訊CPC
W: www.citictel-cpc.com
亞太區: info@citictel-cpc.com
歐洲及CIS: info-eu@citictel-cpc.com

香港 T: 852 2170 7101
日本 T: 81 3 5339 1968
愛沙尼亞 T: 372 622 33 99
台灣 T: 886 2 6600 2588
馬來西亞 T: 603 2280 1500
波蘭 T: 48 22 630 63 30
中國大陸 (Toll Free): 400 651 7550
新加坡 T: 65 6220 6606
荷蘭 T: 31 20 567 2000

TDR2301TC

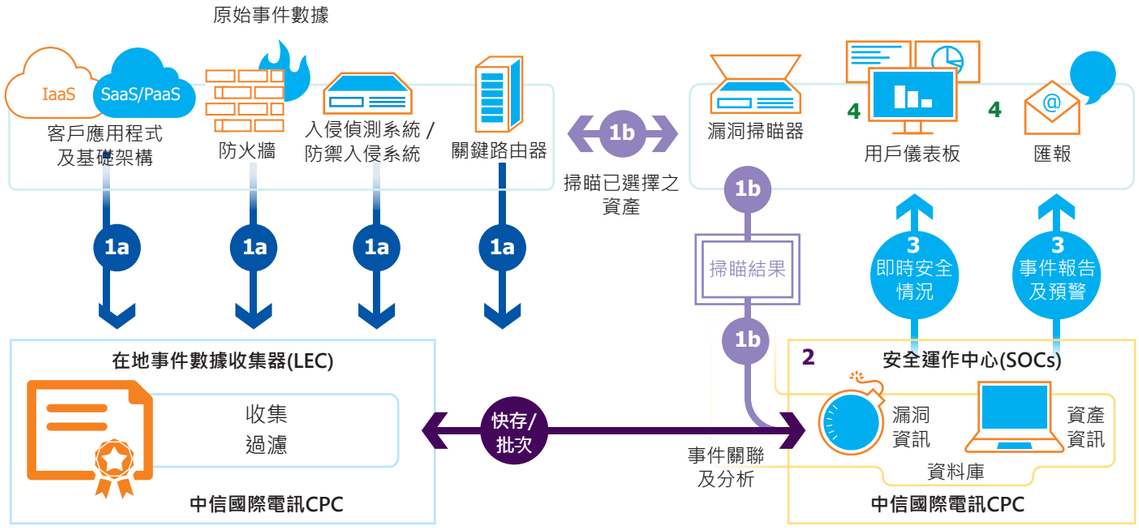
企業隨著數碼轉型策略獲得敏捷性、效率、影響力和競爭力，也變得更容易受到新威脅的攻擊。

為實現更強健的信息安全狀態，全天候且訓練有素的信息安全團隊必不可少。這就是TrustCSI™ 威脅偵測及回應服務的基礎。

中信國際電訊CPC建立了TrustCSI™威脅偵測及回應服務，利用先進的資訊科技信息安全技術，配合中信國際電訊CPC具高度可用性和強大災難恢復功能的多個信息安全營運中心（SOCs），可成為企業全面的資訊科技信息安全專門小組。TrustCSI™威脅偵測及回應服務可在整體企業網絡中提供24x7x365無處不在的可見性，實現更快的威脅偵測及回應，以擊敗網絡罪犯高級嶄新的入侵和偽裝技術，例如打包、加密、多型等。

分析主導型安全性資訊與事件管理技術

新一代安全性資訊與事件管理技術能辨識更廣泛的設備、應用程式、數據來偵測及解決新型入侵性事件。



1a. 原始事件日誌(客戶應用程式及基礎架構、防火牆、入侵偵測系統 / 防禦入侵系統、關鍵路由器等，會被發送到中信國際電訊CPC LEC 進行過濾和聚合，然後傳送給中信國際電訊CPC SOC。

1b. 漏洞掃描器會定期掃描選定的資產，並傳遞掃描結果至知識庫以作存儲。

2. 中信國際電訊CPC SOCs利用SIEM (安全信息及事件管理) 引擎在元日誌與知識庫之間進行關聯及分析，相關結果會被劃分至適當的類別和歸類風險等級。

3. 如果相關信息安全事件的嚴重程度超過正常參數 (與客戶商定) ，中信國際電訊CPC的信息安全專家將啟動事件回應機制，客戶可透過線上終端用戶網上平台 (儀錶板) 查看全部詳細資訊。

4. 線上 TrustCSI™ MSS 網上平台為客戶提供即時信息安全狀態的完整資料，包括完整的信息安全事件處理細節，以及來自世界各地的最新與信息安全相關的 RSS 新聞源。

中信國際電訊CPC的 TrustCSI ™ 威脅偵測及回應服務是世界級的端到端設計而成，並由最佳的人員、流程和技術所支援

專業的信息安全專家團隊

中信國際電訊CPC的安全專家100%通過各種國際安全認證，包括CISA、CISSP以及Comp-TIA Security+，為企業提供最優質的信息安全服務。透過中信國際電訊CPC，亞太區內擁有高超技術及取得各種安全技術認證的安全專家，隨時為各企業效勞。

世界級的安全運作中心(SOCs)

中信國際電訊CPC的安全運作中心獲 ISO9001、ISO14001、ISO20000、ISO27017及ISO27001信息安全管理認證等多項國際認證，並遵行以 ITIL 為本的處理程序， 確保TrustCSI™ 託管式安全服務以業界最佳規範及一致的程序處理威脅事件及政策。

先進的安全信息及事件管理(SIEM)技術

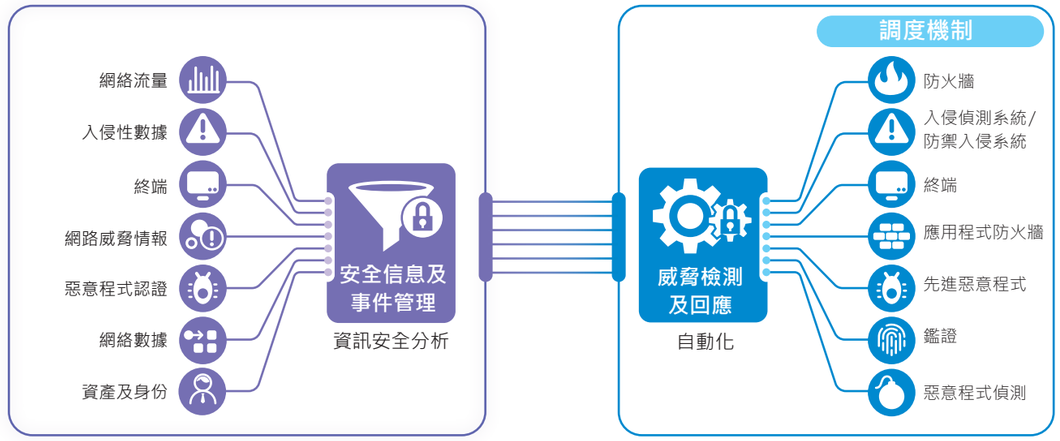
TrustCSI™ 託管式安全服務建基於先進的關聯及分類的安全信息及事件管理(SIEM)引擎。每天追蹤數以十億計事件，及時又準確地確認真正的威脅，令企業可作出快速的修正行動，並大大減少企業分析及關聯安全信息事件的時間。

TrustCSI™ 威脅偵測及回應服務

包括安全事件回應 (IR) 和安全編排及自動化回應 (SOAR) 服務:

威脅檢測及回應服務 (SOAR)

威脅檢測及回應服務（SOAR）是資訊科技安全技術和流程的融合，整合了多個有關警告源和數據的攻擊，然後進行深入分析以確定最佳的補救方法，減輕影響。它利用標準化的工作流程來簡化事件回應的定義、優先順序及驅動，從而精簡流程，而透過自動化手冊，亦可加快回應速度，並減低出錯，從而有效地全面提升效率。中信國際電訊CPC的信息安全專家利用過往真實先例的事件回應製成手冊，在不同客戶的需要時作相關回應，來解決不同的客戶需求。通過 SOAR，能統一作資訊保安控制。



根據預先定義的手冊或工作流程，自動回應信息安全警報，加快事件回應速度。

支援200多個常見品牌資產的整合，包括網路設備、信息安全設備、伺服器、終端、應用程式等。

根據客戶的要求，提供專業定製手冊服務，具有可追蹤及可審核的記錄。

進階月度報告，具備詳細的客製化監控儀表板，易於存取並具有清晰的視覺化呈現。